



OFFICIAL: Sensitive

Digital Device Examination – Copy, transfer, storage and disposal of data

Standard Operating Procedure

Document ID (PPN)	BE-6198
TRIM record number	ADD2024/2270706
BCS Function	Border Enforcement
Document owner	Commander, Technical Support to Operations
Approval date	12 July 2024
Document Contact	Digital Device Examination S. 47E(d) [REDACTED]@abf.gov.au

OFFICIAL: Sensitive

Table of Contents

1. Purpose	3
2. Scope	3
2.1. In Scope	3
2.2. Out of Scope	3
3. Standard Operating Procedure	3
3.1. Copying of Data	3
3.2. Transfer of Copied Data	4
3.3. Storage of Data	4
3.4. Disposal of Data	5
3.5. Record Keeping	5
3.6. Security	6
4. Statement of Expectation	6
5. Accountability and Responsibilities	7
6. Version Control	8
Attachment A – Definitions	9
Attachment B – Assurance and Control Matrix	11
1.1. Powers and Obligations	11
1.2. Controls and Assurance	11
Attachment C – Consultation	13
1.1. Internal Consultation	13
Attachment D – S. 47E(d)	14

1. Purpose

As a result of an electronic device examination a Border Force Officer may copy documents, subject to legislative authority. This Standard Operating Procedure (SOP) outlines the procedure to copy documents as a result of an electronic device examination and the accountability, security and record keeping for the procedure. This SOP must be read in conjunction with the *Electronic Device Examination – Policy Statement (BE-6168)*, *Digital Device Examination – Procedural Instruction (BE-6185)* and *Use of Digital Device Examination to Examine Electronic Devices – Standard Operating Procedure (BE-6197)*.

This SOP provides a system to protect the integrity of documents or electronic records copied and supports officers and the Australian Border Force (ABF) in adhering to legislative and regulatory requirements.

2. Scope

2.1. In Scope

This SOP covers any copying of a document/s or electronic record/s by a Border Force Officer (BFO) as a result of an examination utilising Digital Device Examination (DDE) equipment or capability.

2.2. Out of Scope

Any activity by a Digital Forensic Investigator (DFI) is covered by existing Digital Forensic SOPs and is outside the scope of this document.

It is not intended to summarise or replicate all applicable legislative and regulatory requirements. As a result, it must be read as subject to any applicable laws.

3. Standard Operating Procedure

3.1. Copying of Data

"Copy" is not defined in either the Custom Act, Migration Act or Maritime Powers Act. For the purpose of this document 'to copy' means, "... to make a similar or identical version of; reproduce" a document.

Following the examination and extraction of an electronic device, if a decision is made by the DDE Officer to retain a copy of the device extraction, a copy is to be made of all relevant document/s or electronic records, in the form of one or more extraction files.

If it is decided that a copy is not to be made, or if grounds cannot be located within the extraction that warrant a copy being made, the extraction and all associated files **must** be immediately deleted from the Examination computer.

In the case of a foreign language document, the DDE officer will generally be unable to make a full assessment of the document before it is translated. In such cases the DDE officer should copy the document if they have a reasonable basis for believing it may relate to a relevant offence.

Any copies of extractions through the DDE process are regarded as sensitive and security classified information which must be handled in accordance with current policy guidelines (*refer to Handling Protectively Marked Material – Procedural Instruction (HR-6361)*). If a copy is to be made, the document/s or electronic records **must** be copied while the electronic device is still considered to be under ABF control, once the device is no longer under ABF control or is no longer in a place where ABF holds statutory power a copy can no longer be made.

Should the decision be made to hold a device pending examination, an ABF officer is required to issue a Receipt for Goods (B390) as written notification that their goods have been taken into ABF custody. If required to detain items for examination the appropriate handling guidelines should be followed (refer

OFFICIAL: Sensitive

Detained Goods Management – Procedural Instruction (TT-4786) and/or Evidence Management – Procedural Instruction (BE-2882)).

The document/s or electronic records are to be copied by the DDE Examining Officer to both the designated **Working** and **Backup Storage Solutions**. The Working and Backup Storage Solutions must not exceed security classification level PROTECTED. Any information exceeding this classification should be referred to the work area Officer in Charge (OIC) for handling guidance.

Limited for the purpose of the DDE capability only, departmentally approved external hard drives (HDD) are authorised for the purposes of holding extractions to facilitate operational requirements. These HDD are administered and regulated by Technical Support to Operations (TSO) and referred to as a 'Storage Solution'. All DDE Storage Solution(s) are registered with TSO and provide an encrypted portable **Working** storage system to enable DDE Examining Officers to follow the approved procedure. Additionally, approved HDD's are provided for the Long Term storage of Information, referred to as the **Backup Storage Solution**.

When making a copy of document/s or electronic records relating to the extraction of an electronic device the following information/files **must** be included.

- The original extraction file.
- A Microsoft Excel export of the original extraction file.
- Any photographs taken of the device or material of interest during the examination.

The document/s or electronic records copied are to be checked to ensure there are no errors and the acquired data or extraction is named using the file naming convention outlined in *Use of Digital Device Examination to examine electronic devices – Standard Operating Procedure (BE-6197)*.

After a copy has been made, all files related to the case **must** be immediately deleted from the examination computer.

The excel export of each extractions(s) must then be copied onto the Mobile Phone Data Drop Point (MPDDP). The excel export contains text only data for Intelligence related tasks. The MPDDP is located on a restricted group directory within the ABF Corpnet. The MPDDP is administered by Cyber Risk and Intelligence Division.

Once the excel export of the extractions(s) has been copied to the MPDDP, all files relating to the extraction must be immediately deleted from working storage.

3.2. Transfer of Copied Data

Any copies of extractions through the DDE process are regarded as sensitive and security classified information which must be transferred via a Safe-Hand courier if posting/sending, accompanied by a s. 47E(d) [redacted] where applicable) and, handled in accordance with current policy guidelines (*refer to Handling Protectively Marked Material – Procedural Instruction (HR-6361)*).

The Working and Backup Storage Solutions must not exceed security classification level PROTECTED. Any information exceeding this classification must be referred to the work area OIC for handling guidance.

Any departmental area or external agency requesting a copy of any extracted data **must** provide an encrypted data storage device for the copy to be transferred to.

External agencies requesting a copy of any extracted data must be referred to the work area responsible for making that copy. Any agency requiring a copy of the extractions must complete a 'Transfer of Digital Device Extraction Request' form and this must be saved to s. 47E(d) [redacted] and added to 'Transfer of Digital Device Extraction Register'.

3.3. Storage of Data

The nature of the designated **Working** and **Backup Storage solutions** will be decided upon by TSO.

The Working and Backup Storage Solutions must not exceed security classification level PROTECTED. Any information exceeding this classification should be referred to the work area OIC for handling guidance.

OFFICIAL: Sensitive

Working and Backup Storage Solutions when not in use must be stored in accordance with current policy guidelines (*refer Handling Protectively Marked Material – Procedural Instruction (HR-6361)*).

All copies of electronic devices conducted by Aviation Travellers/Aviation Operations must be stored on the designated backup Storage Solution.

Should a copy of an electronic device be made by any port other than the Major capital airport in the designated region where Aviation Travellers/Aviation Operations operates (such as Maritime Operations), the designated working storage solution containing the document/s or electronic records **must** be sent to the relevant Digital Device Regional Coordinator, accompanied by a s. 47E(d)

The Digital Device Regional Coordinator will then transfer the document/s or electronic records to the designated major capital airport of that designated region. Aviation Travellers will operate a Backup Storage Solution for long term storage before clearing and returning the provided Working Storage Solution (if applicable). This will be accompanied by the completed Receipt for Classified Material (*refer to Attachment D - Receipt for classified material*).

All document/s or electronic records located on backup storage must be kept for a period determined by the Department of Home Affairs (the Department) data retention policy, which is as follows:

- Data related to import/export – 7 years
- Data related to an investigative prosecution – ranges from kept as a historical archive to years depending on the verdict
- Data related to another agency (AFP, DAFF) – 7 years
- Managing movement of seized goods (e.g. transfer logs) – 7 years
- Data related to intel gathering – 5 years.

If data should be held beyond retention periods, approval is required from Records Management.

3.4. Disposal of Data

All working and backup storage solutions, including all copies of electronic devices, should be disposed of after the required retention periods above.

Disposal of extractions from DDE laptops must be completed by the Digital Device Examination Officer (DDEO) that conducts the extraction.

Disposal of extraction copies are to be monitored by Regional Coordinators.

Disposal will consist of the following:

- Delete the extraction from DDE laptop
- Delete the copy of the extraction from HDD
- Shred discs.

3.5. Record Keeping

Once an officer has determined they have the requisite state of mind to enable them to copy a document or electronic record an official record must be made with details of the reasons that led them to form their state of mind and the statutory provision used.

All copies made of **ANY** electronic devices and document/s or electronic records must be recorded as separate entries on the Electronic Device Examination Register and in the DDE Extraction Transfer Register (Refer to *Electronic Device Examination Forms – Supporting Material (BE-6199)*).

Documents required for record keeping purposes for the transfer of copied documents and must be saved in s. 47E(d) are:

S. 47E(d)

Other documents required to be completed

- Notebook entry.

Should this be a duplicate copy of a device extraction, then this must be noted in the “comments” section of the register.

This record keeping is in addition to all standard national and local record keeping procedures, such as the National Intelligence System (NIS), Baggage and Person Search (BPS) etc.

Any Regulation 4A material must have a warning in the file name eg. WARNING CONTAINS REG4A - MELBLOGGSJM110082018

An officer who provides a copy of a device extraction to another section within the Department and/or an external agency must make a record documenting the specifics of the disclosure, including (if relevant) the disclosure grounds under the *Australian Border Force Act 2015* (Cth), *Privacy Act 1988* (Cth) and/or *Migration Act 1958* (Cth).

3.6. Security

Any copies of extractions through the DDE process are regarded as sensitive and security classified information which must be handled in accordance with current policy guidelines (*refer to Handling Protectively Marked Material – Procedural Instruction* (HR-6361)).

The Working and Backup Storage Solutions should/must not exceed security classification level PROTECTED. Any information exceeding this classification must be referred to the work area OIC for handling guidance.

Should portable hard drives be utilised as a working and/or backup storage solution, these must be departmentally issued encrypted hard drives, ordered through the Service Request Catalogue (SRC). Non-departmentally issued and approved portable hard drives/portable storage MUST not be used.

The DDE Laptops are standalone, and must not be connected to any networks at any point.

Should an Encrypted External HDD be used for the storage of acquired or extracted documents/electronic records, it must be kept in a secure location in the work area when not in use, designated by local work area.

Limited for the purpose of the DDE capability only, departmentally approved external hard drives (HDD) are authorised for the purposes of holding extractions to facilitate operational requirements. These HDD are administered and regulated by TSO and referred to as a ‘Storage Solution’. All DDE Storage Solution(s) are registered with TSO and provide an encrypted portable **Working** storage system to enable DDEO’s to follow procedure. Additionally, approved HDD’s are provided for the Long Term storage of Information, referred to as **Backup Storage Solution**.

All external HDDs are accountable assets and have a unique asset number. They must be labelled to clearly identify them as to their purpose. A separate HDD labelled ‘Reg 4A’ must be utilised for all Reg 4A copies.

Any transfer of an encrypted external HDD must be either by hand or via a sealed secure storage case.

4. Statement of Expectation

The APS Code of Conduct states that an APS employee must comply with any lawful and reasonable direction given by someone in the employee’s Agency who has authority to give the direction under subsection 13(5) of the *Public Service Act 1999* (the Public Service Act).

Failure by an APS employee to comply with any direction contained in this SOP document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions under subsection 15(1) of the Public Service Act.

The Secretary's Professional Standards Direction, issued under subsection 55(1) of the *Australian Border Force Act 2015*, (the ABF Act) requires all IBP workers who are not employed under the Public Service Act to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in this SOP document may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

All IBP workers who make decisions or exercise powers or functions under legislation have a duty to do so in accordance with the requirements of the legislation and legal principles.

5. Accountability and Responsibilities

Role	Description
DDE Examining officers	Personally responsible for ensuring their work is performed to the highest standard and complies with all relevant legislation, policies and procedures
Supervisors	Responsible for: - promoting a culture of high quality work output - ensuring team members are aware of relevant legislation, policy and procedures to undertake their duties - supporting the procedural framework.
DDE Regional Co-ordinators / DDE National Co-ordinator	- Responsible for the general support for the DDE capability for ABF operations, excluding second level technical support.
Operational Capability Branch, Major Capability Division	- Responsible for second level technical support for the Standard Operating Environment for the DDE.
Superintendent Special Technical	Responsible for ensuring that: - Digital Device Examination activities are undertaken in accordance with this Procedure - the Procedure is updated as required to reflect emerging risks and areas of priority for Digital Device Examination - the Review Schedule, Register and Supporting Documentation are maintained and updated as appropriate.

6. Version Control

Version number	Date of issue	Author(s)	Brief description of change
v0.1	January 2019	Tactical Capability Branch	Initial draft
v0.2	May 2019	Tactical Capability Branch	Incorporated comments from internal consultation with Operational Commands and PPCF.
V0.3	September 2019	Tactical Capability Branch	Amendments incorporated from ABF Change Control Board submission.
V0.4	April 2020	Tactical Capability Branch	Consultation with internal stakeholders.
V0.5	July 2020	Legal Group	Legal review for legal clearance purpose
V0.6	July 2020	Tactical Capability Branch	Published Version
v.07	March 2024	Technical Support to Operations	Review undertaken – minor edits to incorporate current operational requirements.

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Baggage and Person Search	BPS	The system for recording all examination activity by the ABF relating to incoming and outgoing travellers.
Backup Storage Solution		An authorised and regulated departmental HDD which is encrypted and endorsed by TCB for the purposes of long term storage of extractions to facilitate operational and intelligence requirements.
Copy		To make a similar or identical version or to reproduce a document. “Copy” is not defined in either the Customs Act, Migration Act or the Maritime Powers Act.
Digital Device Examination	DDE	Digital Device Examination uses dedicated hardware and software to examine mobile devices and removable media in the marine domain or at the border to support the Department’s border related functions.
Digital Forensic Investigator	DFI	A Digital Forensic Investigators role is to identify, preserve, analyse and present electronic evidence in a manner that is admissible as evidence in court and they can provide expert testimony in this field and possess qualifications in the field of digital forensics.
Document		As defined by section 4 of the <i>Customs Act 1901</i> , as “including any article or material from which sounds, images or writing is capable of being produced with or without the aid of a computer or some other device”.
Electronic Records		Information stored on electronic devices, such as hard drives, electronic mobile devices, flash storage media and optical media.
External Hard Drive	External HDD	A portable storage device that can be attached to a computer, such as by a Universal Serial Bus (USB) connection.
Extraction		The process of copying accessible electronic records from an electronic device. Extractions may not include all accessible areas of the device.
Evidential Material		Lawfully obtained electronic devices and electronic records that support the Portfolio undertaking its border protection functions including investigations.
Mobile Phone Data Drop Point	MPDDP	A repository for sensitive and official information collected during digital device examination. The MPDDP is located on the Corpnet LAN and is administered by Intelligence division.

OFFICIAL: Sensitive

Term	Acronym (if applicable)	Definition
National Intelligence System	NIS	The primary corporate intelligence reporting system for the Department and the ABF.
Officer In Charge	OIC	Most senior ranking officer delegated to that task for that work area.
Service Request Catalogue	SRC	The ABF online portal used to request assistance from IT services and support regarding departmental hardware and software.
Transfer		The process of creating a digital copy of data that has been retained under legislation for sharing with other law enforcement partners.
Working Storage Solution		An authorised and regulated departmental HDD which is encrypted and endorsed by TCB for the purposes of holding extractions temporarily to facilitate operational requirements.

Attachment B – Assurance and Control Matrix

1.1. Powers and Obligations

Please Note: Staff exercising any powers, delegations or authorisations outlined in this PI (listed here) must check the latest delegation advice on the Intranet or the relevant instrument in LEGEND to ensure they currently hold the applicable power, delegation or authorisation.

Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	Reference (e.g. section)	Section heading/provision description		
<i>Customs Act 1901</i>	186	General powers of examination of goods subject to customs control	No	N/A
	186A	Power to make copies of, and take extracts from, documents in certain circumstances	No	N/A
<i>Migration Act 1958</i>	252	Searches of persons in certain circumstances	No	N/A
<i>Maritime Powers Act 2013</i>	63	Examining things	No	N/A
	65	Copying records or documents	No	N/A

1.2. Controls and Assurance

Related Policy	Electronic Device Examination – Policy Statement (BE-6168)
Procedures / Supporting Materials	Digital Device Examination – Procedural Instruction (BE-6185) Use of Digital Device Examination to examine electronic devices – Standard Operating Procedure (BE-6197) Digital Device Examination – Hardware Maintenance – Standard Operating Procedure (BE-6537) Electronic Device Examination Forms – Supporting Material (BE-6199)
Training/Certification or Accreditation	Officers who have been assessed as competent under the approved DDE training.
Other required job role requirements	Undergo specific training to meet and maintain specified health, psychological and fitness standards in accordance with Directions for Safety Health and Wellbeing.
Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	s. 22(1)(a)(ii), s. 47E(d) @abf.gov.au Digital Device Examination, Technical Support to Operations, Operational Coordination and Planning

OFFICIAL: Sensitive

Escalation arrangements	DDE Regional Co-Ordinator DDE National Co-Ordinator s. 47E(d) @abf.gov.au Inspector Digital Forensics Superintendent Special Technical
Recordkeeping (e.g. system based facilities to record decisions)	Refer section 3.4 Record Keeping of this document. Content Manager (TRIM)
Program or Framework (i.e. overarching Policy Framework or Business Program)	Digital Device Examination – Governance and Quality Checks – Supporting Material (BE-6538)
Job Family Framework Role	Border Enforcement Operations Officer

Attachment C – Consultation

1.1. Internal Consultation

- All staff
- Technical Support to Operations, Operational Planning and Coordination
- Operational Capability Branch, Major Capability Division
- Cyber Risk Services Branch
- ICT Division
- Integrity and Professional Standards Section
- Privacy and Information Disclosure Section
- PPCF Section
- Legal Group

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982



OFFICIAL: Sensitive

Use of Digital Device Examination to examine electronic devices

Standard Operating Procedure

Document ID (PPN)	BE-6197
TRIM record number	ADD2024/2270690
BCS Function	Border Enforcement
Document owner	Commander, Technical Support to Operations
Approval date	12 July 2024
Document Contact	Digital Device Examination S. 47E(d) @abf.gov.au

OFFICIAL: Sensitive

Table of Contents

1. Purpose	3
2. Scope	3
3. Standard Operating Procedure	3
3.1 Device Identification	4
3.2 Data Preservation and Acquisition	4
3.3 Examination and Analysis	4
3.3.1 Digital Device Examination Procedure	4
3.3.2 Removable Data Storage Device Software Applications	6
3.3.3 Removable Data Storage Device Examination Procedure	6
3.4 Record Keeping	7
4. Statement of Expectation	8
5. Accountability and Responsibilities	8
6. Version Control	9
Attachment A – Definitions	10
Attachment B – Assurance and Control Matrix	13
1.1. Powers and Obligations	13
1.2. Controls and Assurance	13
Attachment C – Consultation	15
1.1. Internal Consultation	15
Attachment D – ABF Port Codes	16

1. Purpose

This Standard Operating Procedure (SOP) must be read in conjunction with *Electronic Device Examination – Policy Statement* (BE-6168) and *Digital Device Examination – Procedural Instruction* (BE-6185) and all associated SOPs and Supporting Material and applicable legislation.

These procedures will ensure that any activity undertaken meets accepted best practice for Digital Device Examination (DDE) and any legislative requirements.

DDE activities must only be undertaken by appropriately trained and DDE examining officers using dedicated tools and rigorous procedures in accordance with legislation and electronic evidence handling procedures so as to be admissible as evidentiary material in a court of law.

Examination of electronic devices must not be undertaken by unqualified/untrained persons as such actions can:

- Potentially compromise electronic evidence affecting its admissibility
- Hinder the successful outcome of the Department of Home Affairs (the Department) objectives
- Cause damage to equipment or data resulting in civil claims or litigation against the Department
- Result in failure to bring an investigation to an appropriate conclusion
- Risk damage to the Department's reputation.

This SOP supports the Department's ability to demonstrate the reliability of the electronic evidence.

2. Scope

This SOP applies to all examinations of electronic devices by the Australian Border Force (the ABF) utilising the Digital Device Examination equipment and capability.

Only mobile devices and removable data storage devices are to be examined using the DDE capability.

3. Standard Operating Procedure

Prior to examining a device the DDE examining officer **must** consider

- The ABF Statutory powers for the examination, including any legislated time limitations
- The purpose of the examination, including consultation with the client if necessary
- Whether the DDE examining officer possesses the necessary resources and tools to facilitate the examination, including
 - Software
 - Hardware
 - Cables, and/or
 - Device documentation
- The operational environment the examination is occurring in. If the device belongs to a traveller the officer should consider whether the device should be retained for examination so that the traveller is not unnecessarily delayed. The examination length and comprehensiveness **must** be determined by the operational need, not by external factors such as departing flights.

3.1 Device Identification

DDE Examining officers must only examine mobile devices and removable data storage devices that they have been trained to examine.

DDE Examining Officers encountering devices that they cannot identify, do not know how to operate or are experiencing difficulty in examining should consider requesting these devices be examined by Digital Forensics.

3.2 Data Preservation and Acquisition

All examinations of mobile devices and removable data storage devices **must** be undertaken using DDE hardware and software to ensure the integrity of data and electronic evidence is maintained to the highest level possible.

Ensure appropriate steps are taken to secure electronic devices and electronic records, as follows:

- A Digital Device Examination **must** be considered before a manual examination is attempted
- Mobile devices s. 47E(d) [redacted] prior to any examination
- SIM cards **should** be removed and extracted separately
- Removal of the SIM card is only mandatory s. 47E(d) [redacted] on the device itself
- s. 47E(d) [redacted] **must** be ensured for any connected removable data storage device
- Consider acquiring data from removable storage separately
- Should there be any indication of s. 47E(d) [redacted] the device must be examined by Digital Forensics
- If the device needs to be s. 47E(d) [redacted] then an examination using DDE equipment **must** be attempted.

3.3 Examination and Analysis

3.3.1. Digital Device Examination Procedure

The process for the examination is

- s. 47E(d) [redacted]
- Commence documentation using the Digital Device Examination form, and continue documenting throughout the examination, of information including:
 - Time/Date as displayed on device
 - Manufacturer
 - Model No.
 - Serial No.
 - Capacity
 - International Mobile Equipment Identity (IMEI) / International Mobile Subscriber Identity (IMSI) / Integrated Circuit Card ID (ICCID)
 - PIN / swipe pattern / password / Biometric lock
 - Version of operating system

OFFICIAL: Sensitive

- Location of device
- Device state (on/off)
- List or note all applications currently running in background on the device
- s. 47E(d)
- Unique identifying features
- The condition of the device including damage (all noted damage **must** be reported to a supervisor as soon as practicable)
- Photograph the device, if required. At a minimum record the
 - General device condition (front/rear). If photographing the front of the device no data displayed on a screen is to be recorded
 - Device settings (IMEI/Serial No., etc.)
 - SIM card (with ICCID)
 - Removable memory card (if possible)
- Record chain of custody of the device
- Conduct research (e.g. user manuals, websites, examination tool device guides) for the mobile device to be examined, if necessary and appropriate
- If the device is off
 - Remove and undertake extraction of the SIM card separately from the mobile device handset
 - The SIM card must not be re-inserted until the completion of the examination
 - Turn the device on and undertake an extraction of the handset (as outlined below)
- If the device is on
 - Ensure power is maintained to the mobile device during the entire examination
 - Confirm date and time of the mobile device against a known reference date and time source
 - Remove and undertake extraction of the SIM card separately from the mobile device handset (if not previously undertaken)
 - Unlock device using provided PIN / passcode / pattern / biometric lock, if required and appropriate
 - Determine operating system of device
 - Prepare device for extraction by selecting appropriate options on device s. 47E(d)
 - Connect device to DDE hardware and conduct initial extraction of device using appropriate software and extraction profile. s. 47E(d)
 - Review extracted electronic records for accuracy and completeness against a small selection of original data stored on the mobile device
 - Examine extracted electronic records. Only after this, determine whether seizure or copying of electronic records or device is appropriate and permitted under relevant ABF statutory power (*see sections 186 and 186A of the Customs Act 1901*)
 - Determine whether any further extractions of the device are to be conducted
 - If the device is to be seized or removed from the location, confirm s. 47E(d), and transfer device according to current evidence handling procedures (Refer to *Evidence Management – Procedural Instruction* (BE-2882))

- If extracted electronic records are to be seized, copy data to external storage according to current evidence handling procedures
- If extracted electronic records are to be copied under statutory authority, copy data as per *Digital Device Examination – Copy, transfer, storage and disposal of data – Standard Operating Procedure (BE-6198)*.

3.3.2. Removable Data Storage Device Software Applications

The dedicated DDE computer system (laptop or workstation) is installed with a range of software tools for the examination of removable data storage devices for its border related functions, including:

S. 47E(d)

The dedicated DDE computer also has installed **S. 47E(d)** to ensure the integrity of the device.

3.3.3. Removable Data Storage Device Examination Procedure

The process for the examination is

- Commence documentation, and continue documenting throughout the examination, of information such as:
 - Manufacturer
 - Model No
 - Serial No
 - Capacity
 - Location of device
 - Unique identifying features
 - The condition of the device including damage (all noted damage **must** be reported to a supervisor as soon as practicable)
 - Times including when entered each application/message/conversation, **S. 47E(d)** etc
- Identify data storage device to determine method of reviewing stored data
- Ensure **S. 47E(d)** installed on DDE computer is operational
- Connect device to DDE computer, for example, connect USB device or insert optical storage disc
- Ensure device has been mounted, if not remove and reinsert device. If the problem persists undertake troubleshooting, such as check **S. 47E(d)**, clean optical storage discs, etc. If the problem cannot be rectified consider other alternative actions for the examination of the device, such as:
 - Examination of other devices to determine the likelihood of the device containing prohibited material or relevant information
 - Referral to Digital Forensics for further examination as per *Digital Device Examination – Procedural Instruction (BE-6185)*

OFFICIAL: Sensitive

- Determine the amount of data stored on the device. If the device contains a large visible amount of data consider whether s. 47E(d) of select directories on the device should be undertaken. If the device appears to contain minimal or no data consider the use of the s. 47E(d)
- If the removable data storage device contains data consider undertaking s. 47E(d)
- If applicable, review the results from s. 47E(d)
- Consider the use of s. 47E(d)
- Examine data to determine if prohibited material or relevant information has been located.
- If prohibited material is located, it must be dealt with and handled in accordance with current seizure and evidence handling procedures.
- If information is located consider the need to copy the electronic record/s as outlined in *Digital Device Examination – Copy, transfer, storage and disposal of data – Standard Operating Procedure* (BE-6198).
- If no prohibited material is located or the device is not to be held pending further examination, all removable data storage devices are to be returned to the owner.

During the examination process consideration must be given to the length of time for the examination with regard to:

- The risk indicators leading to the decision to examine the device
- The amount of data apparent on the removable data storage device
- The length of time required for the s. 47E(d)

3.4. Record Keeping

It is critical that DDE examining officers make contemporaneous notes in a form that enables them to compile reports, statements, conduct interviews and, if required, be used as evidence in a Court of Law. Contemporaneous notes are to be made in a DDE examining officer's official notebook and on an approved Digital Device Examination Form.

If a DDE examining officer uses an ABF statutory power in relation to the examination of an electronic device, an official record **must** be made with details of the reasons that led them to form their state of mind and the statutory power used, such as subparagraph 186A(1)(b)(i) of the *Customs Act 1901* (the Customs Act).

For the purposes of DDE **all** examinations **must** be recorded on the Electronic Device Examination Register and contemporaneously on an approved Digital Device Examination Form. See *Electronic Device Examination Forms – Supporting Material* (BE-6199). They must also be entered into Baggage and Person Search (BPS), where available.

There is to be a separate Digital Device Examination Form for every device examined (note: components of a device can be included on the same form, for example mobile device handset, SIM card, removable storage card).

This record keeping is in addition to all standard national and local record keeping procedures, such as the National Intelligence System (NIS).

Should electronic records be copied under an ABF statutory power, such as section 186A of the Customs Act, the copied data must be recorded consistently with the recording of mobile device acquisitions/extractions, including copying the excel export of each extractions(s) onto the Mobile Phone Data Drop Point (MPDDP) as per *Digital Device Examination – Copy, transfer, storage and disposal of data – Standard Operating Procedure* (BE-6198).

Should the decision be made to hold a device pending examination, a DDE examining officer is required to issue a Receipt for Goods (B390) to the person purporting to be the owner of the device as written notification that their goods have been taken into ABF custody. If devices are held for examination, the appropriate handling guidelines should be followed (refer *Detained Goods Management – Procedural Instruction* (TT-4786) and/or *Evidence Management – Procedural Instruction* (BE-2882)).

OFFICIAL: Sensitive

An electronic Case folder is to be created in the format: "YYYY-MM-DD_SURNAME, Given Names (Sex) DOB (DDMMYYYY)" Eg. 2018-08-10_BLOGGS, Joe (M) DOB 28AUG1999

Sub directories (exhibits) are to be created for individual data storage devices. Use the following convention for naming the individual data storage device directories for copied electronic record/s or documents including any photographs taken:

Port Code	Surname	Initial(s)	Device		Examination Date (DDMMYYYY)
			Type	Number	
MEL	BLOGGS	J	M	1	10082018

- **Port Code:** As per Attachment D (ABF Port Codes)
- **Device type:** M – Mobile device S – SIM card D – Data storage device
- **Device number:** If the traveller has more than one device, insert the number appropriately – e.g. M2, M3, etc.

This naming convention must be used for recording purposes for all official records and databases:

PORTCODESURNAMEINITIAL/SDEVICETYPENUMBERDATE(DDMMYY) eg. MELBLOGGSJM110082018

4. Statement of Expectation

The APS Code of Conduct states that an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction under subsection 13(5) of the *Public Service Act 1999* (the Public Service Act).

Failure by an APS employee to comply with any direction contained in this SOP document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions under subsection 15(1) of the Public Service Act.

The Secretary's Professional Standards Direction, issued under subsection 55(1) of the *Australian Border Force Act 2015*, (the ABF Act) requires all IBP workers who are not employed under the Public Service Act to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in this SOP document may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

All IBP workers who make decisions or exercise powers or functions under legislation have a duty to do so in accordance with the requirements of the legislation and legal principles.

5. Accountability and Responsibilities

Role	Description
DDE Examining officers	Appropriately trained and skilled ABF officers, who are personally responsible for ensuring their work is performed to the highest standard and complies with all relevant legislation, policies and procedures.

Role	Description
Supervisors	Responsible for: - promoting a culture of high quality work output - ensuring team members are aware of relevant legislation, policy and procedures to undertake their duties - supporting the procedural framework.
DDE Regional Co-ordinators / DDE National Co-ordinator	Responsible for the general support for the DDE capability for ABF operations, excluding second level technical support.
Operational Capability Branch, Major Capability Division	Responsible for second level technical support for the Standard Operating Environment for the DDE capability.
Superintendent Digital Forensic Operations	Responsible for ensuring that: - DDE activities are undertaken in accordance with this SOP - the SOP is updated as required to reflect emerging risks and areas of priority for the DDE - the Review Schedule, Register and Supporting Documentation are maintained and updated as appropriate.

6. Version Control

Version number	Date of issue	Author(s)	Brief description of change
v0.1	February 2019	Tactical Capability Branch	Initial draft
v0.2	May 2019	Tactical Capability Branch	Incorporated comments from internal consultation with Operational Commands and PPCF.
V0.3	September 2019	Tactical Capability Branch	Amendments incorporated from ABF Chang Control Board submission
V0.4	April 2020	Tactical Capability Branch	Internal consultation.
V0.5	July 2020	Legal Group	Legal review for clearance purposes.
V0.6	July 2020	Tactical Capability Branch	Published Version
v.07	March 2024	Technical Support to Operations	Review undertaken – minor edits to incorporate current operational requirements.

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Acquisition		A device incorporating all accessible sectors or blocks, including unallocated sectors.)
Baggage and Person Search	BPS	The system for recording all examination activity by the ABF relating to incoming and outgoing travellers.
Biometric lock		A type of security lock set by the user to prevent access to the device that involves a biometric scanning a fingerprint or facial recognition to unlock the device.
Case Officer		The person requesting the electronic device examination or the person representing that person.
Copy		To make a similar or identical version or to reproduce a document. "Copy" is not defined in either the Customs Act, Migration Act or the Maritime Powers Act.
Digital Device Examination	DDE	Digital Device Examination uses dedicated hardware and software to examine mobile devices and removable data storage devices in the marine domain or at the border to support the Department's border related functions.
Document		As defined by s.4 of the <i>Customs Act 1901</i> , as "including any article or material from which sounds, images or writing is capable of being produced with or without the aid of a computer or some other device".
Electronic evidence		Lawfully obtained electronic records that are relevant to an investigation. In this SOP this term also includes lawfully obtained electronic records that support the ABF undertaking its border protection functions.
Electronic Records		Information/data stored on electronic devices, such as hard drives, electronic mobile devices, flash storage media and optical media. Information stored on electronic devices, such as hard drives, electronic mobile devices and flash storage. Generally may fall under the definition of 'document' in section 4 of the <i>Customs Act 1901</i> , which includes: - any paper or other material on which there is writing; and - any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and - any paper or other material on which a photographic image or any other image is recorded; and

OFFICIAL: Sensitive

Term	Acronym (if applicable)	Definition
		any article or material from which sounds, images or writing is capable of being produced with or without the aid of a computer or some other device.
Extraction		The process of copying accessible electronic records from an electronic device. Extractions may not include all accessible areas of the device.
Integrated Circuit Card ID	ICCID	The unique serial number assigned to, maintained within, and usually imprinted on the (U)SIM.
International Mobile Equipment Identity	IMEI	A unique identification number programmed into GSM and UMTS mobile devices.
International Mobile Subscriber Identity	IMSI	A unique number associated with every GSM mobile phone subscriber, which is maintained on a (U)SIM.
s. 47E(d)		s. 47E(d)
Mobile device		A portable computing device such as a smartphone or tablet computer excluding laptop computers.
National Intelligence System	NIS	The primary corporate intelligence reporting system for the Department and the ABF.
Personal Identification Number	PIN	A setting that may be enabled on devices or SIM cards to provide security for the device. If a PIN is enabled, the user will need to enter the PIN to unlock the device.
Passcode		A password code set by the user to prevent access to the device that involves entering the passcode to unlock the device.
Swipe pattern		A type of security lock set by the user to prevent access to the device that involves drawing a pattern to unlock the device.
Prohibited material		Includes: - prohibited imports, such as material falling under regulation 4A of the <i>Customs (Prohibited Imports) Regulations 1956</i>; and - restricted goods, as prescribed in regulation 131 of the <i>Customs Regulation 2015</i>.
Removable data storage device		A data storage device designed to be inserted and removed from a system, which can be used for storing and transporting data. Data storage device is defined in section 183UA of the <i>Customs Act 1901</i> to mean a thing containing, or designed to contain, data for use by a computer. For example, an external hard drive.

OFFICIAL: Sensitive

Term	Acronym (if applicable)	Definition
Subscriber Identity Module	SIM	The card used in some devices that allows the device to connect to a carrier network (Telstra, Optus, Vodafone, etc.). SIM cards may contain identifying information and other data.
Transfer		The process of creating a digital copy of data that has been retained under legislation for sharing with other law enforcement partners.
s. 47E(d)		s. 47E(d)
s. 47E(d)		s. 47E(d)

Attachment B – Assurance and Control Matrix

1.1. Powers and Obligations

Please Note: Staff exercising any powers, delegations or authorisations outlined in this PI (listed here) must check the latest delegation advice on the Intranet or the relevant instrument in LEGEND to ensure they currently hold the applicable power, delegation or authorisation.

Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	Reference (e.g. section)	Section heading/provision description		
<i>Customs Act 1901</i>	s186	General powers of examination of goods subject to customs control	No	N/A
	s186A	Power to make copies of, and take extracts from, documents in certain circumstances	No	N/A
<i>Migration Act 1958</i>	s252	Searches of persons in certain circumstances	No	N/A
<i>Maritime Powers Act 2013</i>	s63	Examining things	No	N/A
	s65	Copying records or documents	No	N/A

1.2. Controls and Assurance

Related Policy	Electronic Devices Examination – Policy Statement (BE-6168)
Procedures / Supporting Materials	Digital Device Examination – Procedural Instruction (BE-6185) Digital Device Examination – Copy, transfer, storage and disposal of data – Standard Operating Procedure (BE-6198) Electronic Device Examination Forms – Supporting Material (BE-6199)
Training/Certification or Accreditation	Officers who have been assessed as competent under the approved DDE training.
Other required job role requirements	BFO Foundation Module – Compile and Use Official Notes BFO Foundation Module –Examine Goods & Copy Docs s186/186A BFO Foundation Module – State of Mind BFO Foundation Module – Manage Physical Evidence
Other support mechanisms (e.g. who can provide further assistance in relation to any aspects of this instruction)	S. 47E(d) @abf.gov.au Digital Forensic Operations, Technical Support to Operations

OFFICIAL: Sensitive

Escalation arrangements	DDE Regional Co-Ordinator DDE National Co-Ordinator S. 47E(d) @abf.gov.au Inspector Digital Forensics Superintendent Digital Forensic Operations
Recordkeeping (e.g. system based facilities to record decisions)	Refer section 3.4 <i>Record Keeping</i> of this document. Content Manager (TRIM)
Program or Framework (i.e. overarching Policy Framework or Business Program)	Digital Device Examination – Governance and Quality Checks – Supporting Material (BE-6538)
Job Family Framework Role	Border Enforcement Operations Officer

Attachment C – Consultation

1.1. Internal Consultation

- All staff
- Technical Support to Operations, Operational Coordination and Planning
- Operational Capability Branch, Major Capability Division
- Cyber Risk Services Branch
- ICT Division
- Integrity and Professional Standards
- Privacy and Information Disclosure Section
- PPCF Section
- Legal Group

Attachment D – ABF Port Codes

ABF Port Codes							
ACT		Gove	GOV	Edinburgh Airport	EBH	Melbourne Airport	MAP
Canberra	CBR	Tindal	TIN	Edithburg	EDB	Portland	PAD
Canberra Airport	CAN	QLD		Nuriootpa	NRP	Tullamarine	TME
ACT Parcels Post	APP	Abbot Point	ABP	Port Adelaide	PAE	Vic Parcels Post	VPP
NSW		Amberley Airport	ABL	Port Augusta	PUG	Welshpool	WEL
Albury Wodonga	ABX	Bowen	ZBO	Port Bonython	PBY	Westernport	WEP
Bankstown	BWU	Brisbane	BNE	Port Lincoln	PLO	WA	
Coffs Harbour	CFS	Bundaberg	BDB	Port Pirie	PPI	Albany	ALH
Eden	QDN	Cairns	CNS	Port Stanvac	PST	Bunbury	BUY
Grafton	GFN	Cairns Airport	CRN	Rapid Bay	RAB	Busselton	BUS
Griffith	GFF	Coolangatta Airport	OOL	SA Parcel Post	SAP	Broome	BME
Kurnell	KUR	Gladstone	GLT	Wallaroo	WAL	Cape Cuvier	CCU
Lord Howe Island	LDH	Hamilton Island	HTI	Whyalla	WYA	Carnarvon	CVQ
Mascot	MAS	Haypoint	HYP	TAS		Christmas Island	CHI
Newcastle	NTL	Innisfail	IFL	Bell Bay	BEL	Cocos Island	CCI
NSW Parcel Post	NPP	Karumba	KRB	Burnie	BWT	Dampier	DAM
Nowra	NOA	Lucinda	LUC	Devonport	DPO	Derby	DRB
Parramatta	PRM	Mackay	MKY	Hobart	HBA	Esperance	EPR
Port Botany	PTB	Maroochydore Airport	MCY	Hobart Airport	HBT	Exmouth	PEX
Port Kembla	PKL	Maryborough	MBH	Launceston	LST	Fremantle	FRE
Richmond	RCH	Proserpine Airport	PPP	Naracoopa	NCP	Geraldton	GET
Richmond Airport	RIC	QLD Parcels Post	QPP	Port Latta	PLA	Onslow	ONS
Sydney	SDN	Rockhampton	ROK	Port Stanley	PSY	Pearce Airport	PCE
Sydney Airport	SYD	Thursday Island	TIS	Spring Bay	SPB	Port Headland	PHE
Trial Bay	TRB	Townsville/Airport	TSV	Ulverstone	ULV	Port Sampson	SPP
Williamtown Airport	WST	Weipa	WEI	VIC		Port Walcott	PWL
NT		SA		Albury Wodonga	ABX	Perth/Airport	PER
Alice Springs	ASP	Adelaide	ADL	Avalon Airport	AVV	Useless Loop	USL
Ayers Rock	AYQ	Adelaide Airport	ADA	East Sale	SXE	WA Parcels Post	WPP
Darwin	DRW	Ardrossan	ARD	Essendon Airport	MEB	Wyndham	WYD
Darwin Airport	DAA	Berri	BER	Geelong	GEX	Yampi Sound	YAM
Groote Eylandt	GTE	Cape Thevenard	THE	Melbourne	MEL	Offshore	OFF



Australian Government
Department of Home Affairs

OFFICIAL: Sensitive

Electronic Device Examination Forms

Supporting Material

Elec

Document ID (PPN)	BE-6199
TRIM record number	ADD2024/2270727
BCS Function	Border Enforcement
Document owner	Commander, Technical Support to Operations
Approval date	12 July 2024
Document Contact	Digital Device Examination S. 47E(d) @abf.gov.au

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL: Sensitive

Table of Contents

1. Introduction	3
2. Examination Forms	3
2.1. Digital Device Examination Form	3
2.2. Manual Device Examination Form	3
2.3. Electronic Device Examination Register	3
2.4. Digital Device Examination Re-imaging Register	3
2.5. Transfer of Digital Device Extraction Register	3
2.6. Transfer of Digital Device Extraction Request	3
3. Version Control	3
Attachment A – Digital Device Examination Form	4
Attachment B – Manual Device Examination Form	6
Attachment C – Electronic Device Examination Register	9
Attachment D – Digital Device Examination Re-imaging Register	10
Attachment E – Transfer of Digital Device Extraction Register	11
Attachment F – Transfer of Digital Device Extraction Request	12

1. Introduction

This Supporting Material provides the forms to be used for the examination of electronic devices by the Digital Device Examination (DDE) capability and for the manual examination of devices by all Australian Border Force officers, except Digital Forensic Investigators (DFI's).

These forms are to be completed as outlined in their relevant Procedural Instructions and Standard Operating Procedure/s.

2. Examination Forms

2.1. Digital Device Examination Form

See Attachment A.

2.2. Manual Device Examination Form

See Attachment B.

2.3. Electronic Device Examination Register

See Attachment C.

2.4. Digital Device Examination Re-imaging Register

See Attachment D.

2.5. Transfer of Digital Device Extraction Register

See Attachment E.

2.6. Transfer of Digital Device Extraction Request

See Attachment F.

3. Version Control

Version number	Date of issue	Author(s)	Brief description of change
V0.1	March 2020	Tactical Capability Branch	Initial draft
V0.2	May 2020	Tactical Capability Branch	Comments incorporated from internal consultation from Operational Commands and PPCF
V0.3	July 2020	Legal Group	Legal review for legal clearance purpose.
V0.4	July 2020	Tactical Capability Branch	Published Version
v0.5	March 2024	Technical Support to Operations	Review undertaken – minor edits to incorporate current operational requirements.

Attachment A – Digital Device Examination Form



Australian
BORDER FORCE

Protected (when completed)

Digital Device Examination

FAMILY NAME, Given Name(s), Gender, DOB				Flight Number or Vessel Name				Passport Number					
s. 47E(d)				s. 47E(d)				Location of Examination					
Received From (Officer User ID or Pax)				Device Received (Time / Date) : / /				Device Returned (Time / Date) : / /					
Returned to (Officer User ID or Pax)				Digital Device Examination Officer (User ID)				Condition of Device (if scratched / damaged / photographs, if taken)					
Equipment * Use ONE form for EACH DEVICE – for MULTIPLE DEVICES attach ALL forms together for EACH PAX *													
DEVICE		Mobile Phone - Tablet - SIM - DSC						Extraction Start Time		:	Extraction End Time		
Make / Model (include model number and capacity)						Phone Number (if available)							
IMEI / IMEI's / MEID (from handset s. 47E(d)) IMEI 1: IMEI 2: MEID:						Device Security Code or Swipe Pattern ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Fingerprint: Yes No							
Serial No.				Manual Exam Prior		Yes No							
Operating System / Version		Phone Power		On Off Time:		Battery Present		Yes No		s. 47E(d) Yes No Time:			
s. 47E(d)		s. 47E(d)		On Off Time:		s. 47E(d)		On Off Time:		Removed SIM/SIMS Yes No			
SIM Card		Yes No		Examined separately		Yes No		Extraction Start Time		:	Extraction End Time		
Card Issuer / Carrier				PIN		IMSI s. 47E(d)				ICCID (from SIM s. 47E(d))			
Data Storage Card (DSC)		Yes No		Examined separately		Yes No		Extraction Start Time		:	Extraction End Time		
Type		Brand		Capacity		s. 47E(d)							
Examination Summary													
Mobile Device Extraction (MDE) Method(s)		s. 47E(d)		Extraction Profile used									
Extraction(Ext) Successful		Yes No		Ext. Aborted		Yes No		Abort Reason					
Exam Data Retained		Yes No		Reason(s) if data copied under section 186A		(Further details on additional notes page if required)							
Photographs Taken		Yes No		Photographs Retained		Yes No		Photographs added to (circle)		s. 47E(d) CASE FILE			
File name(s) Include SIM or DSC if applicable													
File(s) s. 47E(d) file included in exam data		Yes No		Report to Intel Drop Point		Yes No		User ID		Time / Date			
Technical issues (not supported, supported but problem, cable, computer)													

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL: Sensitive

Additional Notes		
Date	Time	DETAILS: S. 47E(d) reason for manual examination prior to DDE examination (<i>Attach Manual Examination form</i>), change of custody during extraction from one DDE Officer to another, photographs (if taken), details and times of classification of images (terrorism, child exploitation, money laundering etc.)
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		

External Hard Drive / USB Drive (or CD/DVD) Transfer				
Date	Time	From	To	Comments
/ /				
/ /				
/ /				
/ /				

Device Custody (if required)				
Date	Time	From	To	Comments (including barcodes)
/ /				
/ /				
/ /				

Further Action				
Device held on B390 for further examination	Yes	No	Details (include B390 S. 47E(d) Infringement Numbers)	
Device seized	Yes	No		
Device referred to ABF Investigations	Yes	No		
Device referred to other agency	Yes	No		
NIS Report	Yes	No	NIS Number:	
Examining Officer's Name, Signature & Date				
/ /				

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Attachment B – Manual Device Examination Form

PROTECTED (WHEN COMPLETED)

WARNING: Consider that due to the risks associated with a manual examination, DFI may refuse any referral of the digital device.



Australian
BORDER FORCE

Manual Device Examination

FAMILY NAME, Given Name(s), Gender, DOB		Flight Number or Vessel Name	Passport Number
s. 47E(d)	s. 47E(d)	Location of Examination	
Received From (Officer User ID or Pax)	Device Received (Time / Date)	Device Returned (Time / Date)	Returned to (Officer User ID or Pax)
Manual Examination Officer (User ID)		Condition of Device (if scratched / damaged / photographs, if taken)	

Equipment * Use ONE form for EACH DEVICE – for MULTIPLE DEVICES attach ALL forms together for EACH PAX *

Device	Mobile Phone	Tablet		Examination Start Time	:	Examination End Time	:									
Make / Model and number / Operating System and Version / Capacity				Phone Number (if available)												
IMEI / IMEI's list below IMEI 1: IMEI 2: MEID: Serial Number:				Device Security Code or Swipe Pattern <table border="0"> <tr><td>○</td><td>○</td><td>○</td></tr> <tr><td>○</td><td>○</td><td>○</td></tr> <tr><td>○</td><td>○</td><td>○</td></tr> </table> Fingerprint: Yes No				○	○	○	○	○	○	○	○	○
○	○	○														
○	○	○														
○	○	○														

Applications running in background:

Reason why DDE capability not used:

Any s. 47E(d) - list below	DDE exam attempted	Yes No	All risks considered	Yes No	s. 47E(d)	Yes No Time:
	s. 47E(d)	On Off Time:	s. 47E(d)	On Off Time:	Removed SIM/SIMS	Yes No

Photographs Taken	Yes No	Photographs Retained	Yes No	Photographs added to (Circle)	s. 47E(d)	CASE FILE
-------------------	--------	----------------------	--------	-------------------------------	-----------	-----------

Date	Time	Details: Time s. 47E(d), including legislation, issues, images captured – times and classification of images (terrorism, child exploitation, money laundering etc.)
/ /		
/ /		
/ /		
/ /		
/ /		
/ /		
Date	Time	Details (Continued):

Released by Department of Home Affairs under the Freedom of Information Act 1982

OFFICIAL: ~~Sensitive~~

[illegible]

External Hard Drive / USB Drive (or CD/DVD) Transfer

Date	Time	From	To	Comments
/ /				
/ /				
/ /				

Further Action

Device held on B390 for further examination	Yes	No	Details (include B390 § 47E(0) Infringement Numbers)
Device seized	Yes	No	
Device referred to ABF Investigations	Yes	No	
Device referred to other agency	Yes	No	
NIS Report	Yes	No	NIS number:
Manual Examination Officer's Name, Signature & Date			
/ /			

Additional Notes page if required

OFFICIAL: Sensitive

[illegible]

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Attachment C – Electronic Device Examination Register

S. 47E(d)

Attachment D – Digital Device Examination Re-imaging Register

S. 47E(d)

Attachment E – Transfer of Digital Device Extraction Register

S. 47E(d)

Attachment F – Transfer of Digital Device Extraction Request



**Australian
BORDER FORCE**

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

S. 47E(d)

Released by Department of Home Affairs
under the Freedom of Information Act 1982